FIG. 1

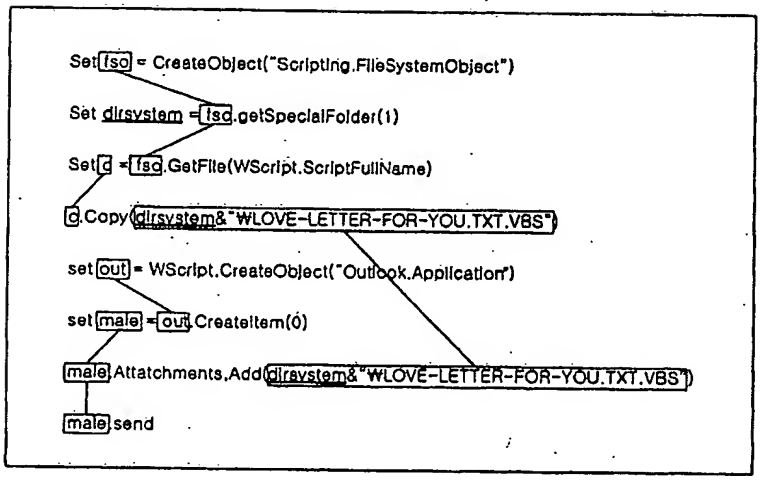

FIG. 2

```
M1 : Set $1 = CreateObject(Scripting.FileSystemObject)
M2 : Set $1 = $2.GetFile(WScript.ScriptFullName)
M3 : $1.Copy($2)

M4 : set $1 = WScript.CreateObject(Outlook.Application)
M5 : set $1 = $2.CreateItem(0)
M6 : $1.Attatchments.Add($2)
M7 : $1.send

R1 : (M1.$1 == M2.$2) && (M2.$1 == M3.$1)
       => $1 = M3.$2                  // code writing
R2 : (M4.$1 == M5.$2) && (M5.$1 == M6.$1) && (M5.$1 == M7.$1)
       => $1 = M6.$2                  // send mail
R3 : R1.$1 == R2.$1
       => $1 = true                   // A Malicious Behavior Is Detected!
```

FIG. 3

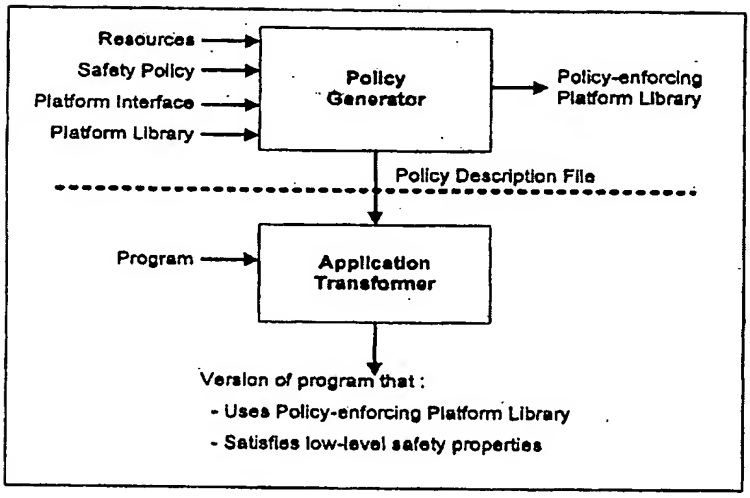
Resources
Safety Policy
Platform Interface
Platform Library
Policy Generator
Policy-enforcing Platform Library
Policy Description File
Program
Application Transformer
Version of program that :
- Uses Policy-enforcing Platform Library
- Satisfies low-level safety properties

FIG. 4

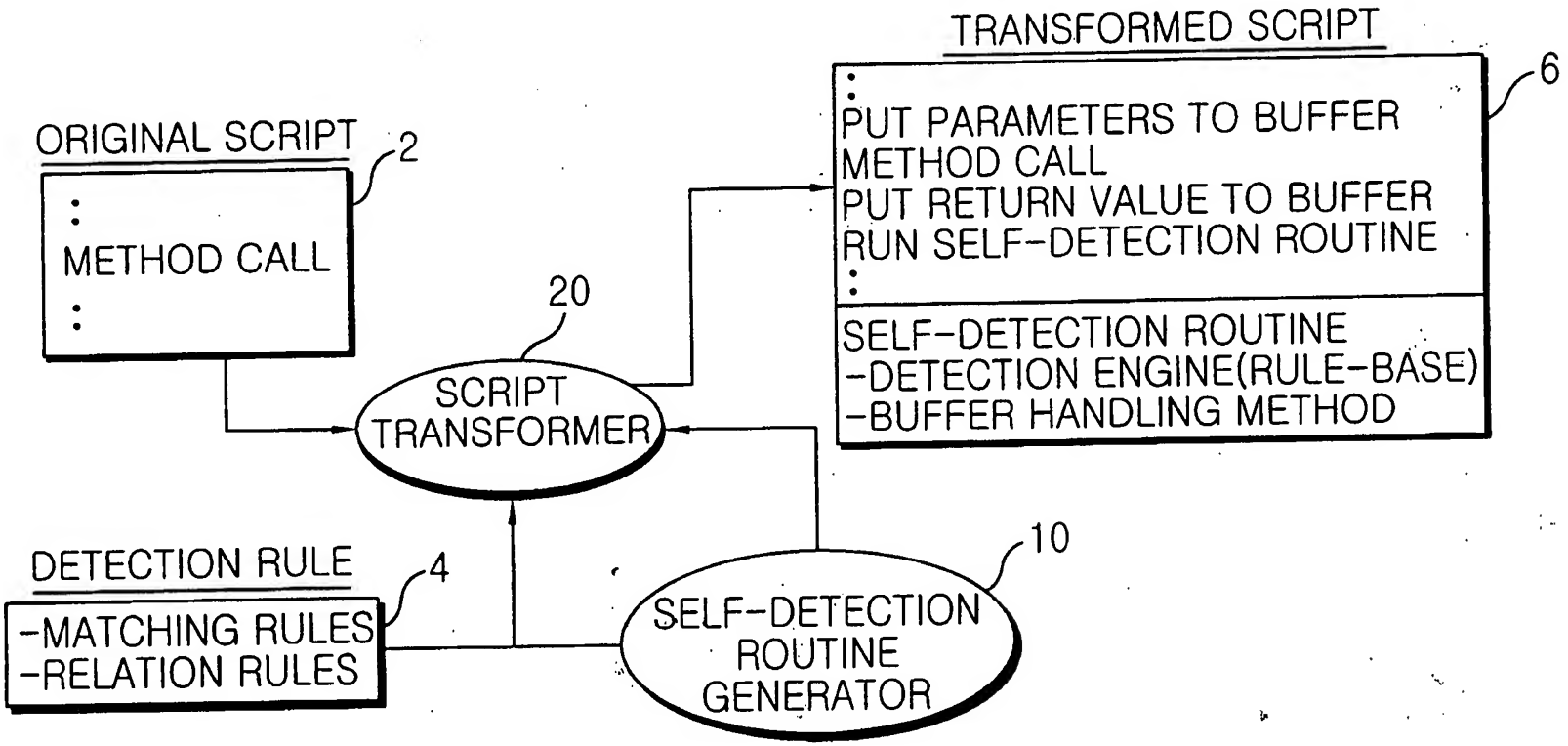
TRANSFORMED SCRIPT
6
:
PUT PARAMETERS TO BUFFER
METHOD CALL
PUT RETURN VALUE TO BUFFER
RUN SELF-DETECTION ROUTINE
:
SELF-DETECTION ROUTINE
-DETECTION ENGINE(RULE-BASE)
-BUFFER HANDLING METHOD
ORIGINAL SCRIPT
2
:
METHOD CALL
:
20
SCRIPT TRANSFORMER
DETECTION RULE
4
-MATCHING RULES
-RELATION RULES
10
SELF-DETECTION ROUTINE GENERATOR

FIG. 5

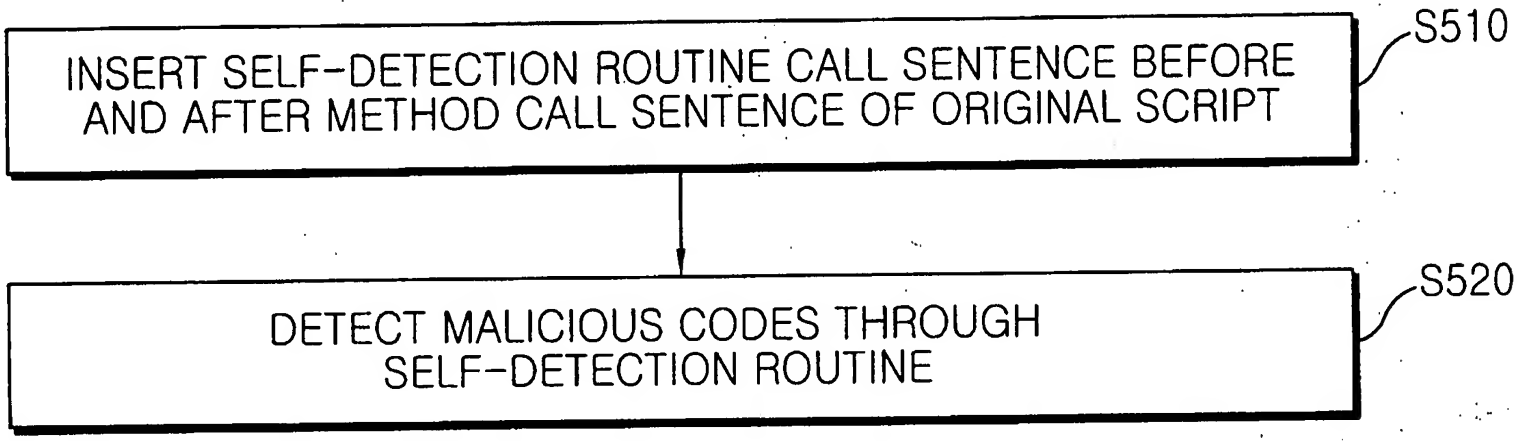
INSERT SELF-DETECTION ROUTINE CALL SENTENCE BEFORE AND AFTER METHOD CALL SENTENCE OF ORIGINAL SCRIPT
S510
DETECT MALICIOUS CODES THROUGH SELF-DETECTION ROUTINE
S520

FIG. 6

```
rule_description ::= ( rule )1.
rule ::= rule_identifier : rule_body
rule_body ::= matching_rule_body | ( relation_rule_body )1.
matching_rule_body ::= script statement with variable_string
variable_string ::= variable | *
variable ::= $ ( digit )1.
relation_rule_body ::= condition_phrase => action_phrase
condition_phrase ::= condition_expr ( logical_operator condition_expr )0.
condition_expr ::= rule_identifier | local_variable string_compare_operator local_variable
logical_operator ::= && | ||
string_compare_operator ::= < | ==
action_phrase ::= action_stmt ( , action_stmt )0.
action_stmt ::= variable = rvalue
rvalue ::= local_variable | variable | true | false
local_variable ::= rule_identifier . variable
```

FIG. 7

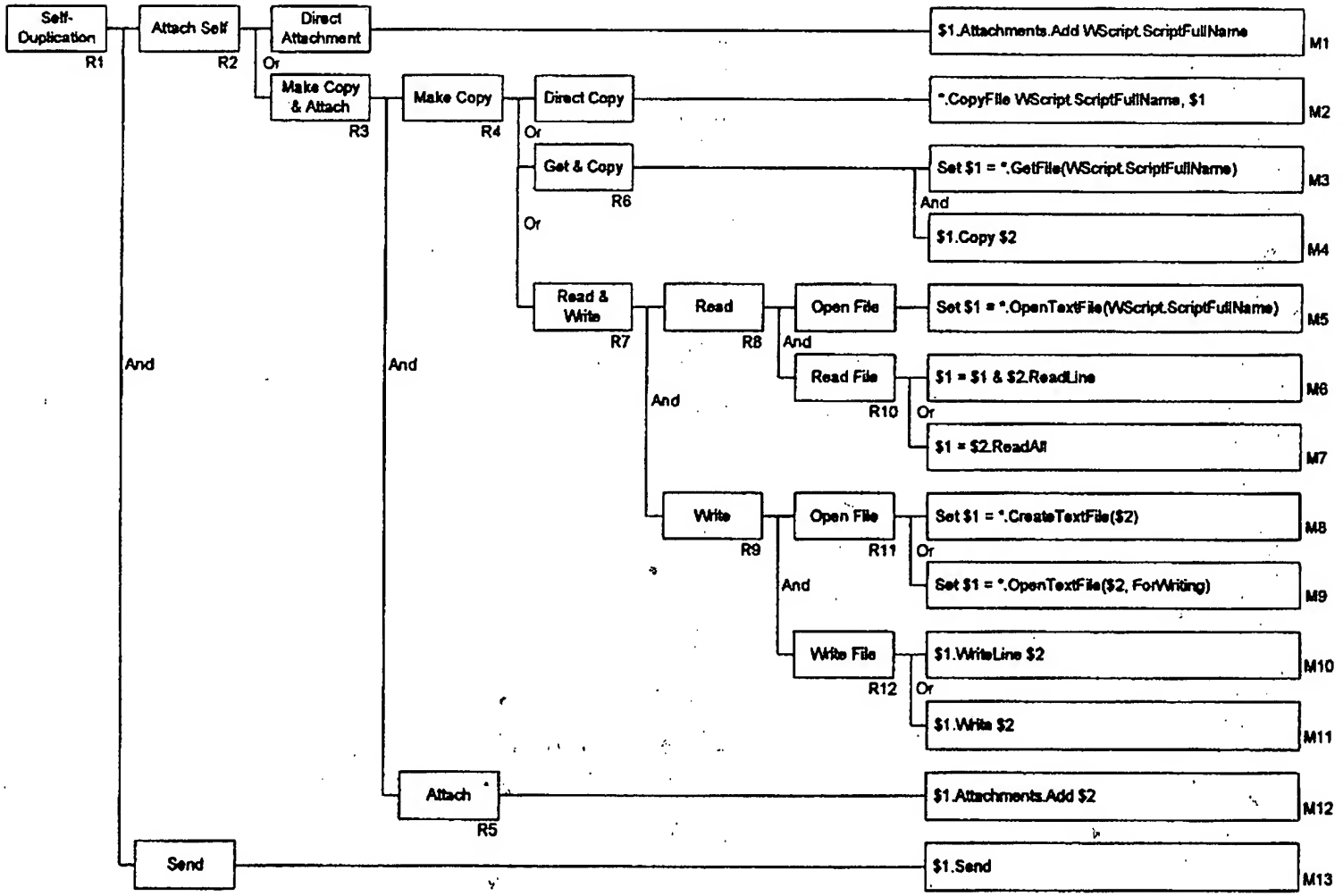
Self-Duplication
R1
Attach Self
R2
Direct Attachment
Or
Make Copy & Attach
R3
Make Copy
R4
Direct Copy
Or
Get & Copy
R6
Or
Read & Write
R7
Read
R8
Open File
And
Read File
R10
Or
And
Write
R9
Open File
R11
Or
And
Write File
R12
Or
And
And
Attach
R5
Send
$1.Attachments.Add WScript.ScriptFullName
M1
".CopyFile WScript.ScriptFullName, $1
M2
Set $1 = ".GetFile(WScript.ScriptFullName)
M3
And
$1.Copy $2
M4
Set $1 = ".OpenTextFile(WScript.ScriptFullName)
M5
$1 = $1 & $2.ReadLine
M6
$1 = $2.ReadAll
M7
Set $1 = ".CreateTextFile($2)
M8
Set $1 = ".OpenTextFile($2, ForWriting)
M9
$1.WriteLine $2
M10
$1.Write $2
M11
$1.Attachments.Add $2
M12
$1.Send
M13

FIG. 8

```
R1  : R2.$1 == M13.$1
      -> $1 = true
R2  : M1 || R3
      -> $1 = $1
R3  : R4.$1 == R5.$2
      -> $1 = R5.$1
R4  : M2 || R6 || R7
      -> $1 = $1
R5  : M12
      -> $1 = $1, $2 = $2
R6  : M3.$1 == M4.$1
      -> $1 = M4.$2
R7  : R8.$1 == R9.$2
      -> $1 = R9.$1
R8  : M5.$1 == R10.$2
      -> $1 = R10.$1
R9  : R11.$1 == R12.$1
      -> $1 = R11.$2, $2 = R12.$2
R10 : M6 || M7
      -> $1 = $1, $2 = $2
R11 : M8 || M9
      -> $1 = $1, $2 = $2
R12 : M10 || M11
      -> $1 = $1, $2 = $2
```

FIG. 9

```
RuleBase.SetVal 0, "M2" : RuleBase.SetVal 2, FSO
Set c = FSO.GetFile(WScript.ScriptFullName)
RuleBase.SetVal 1, c : RuleBase.Check
```
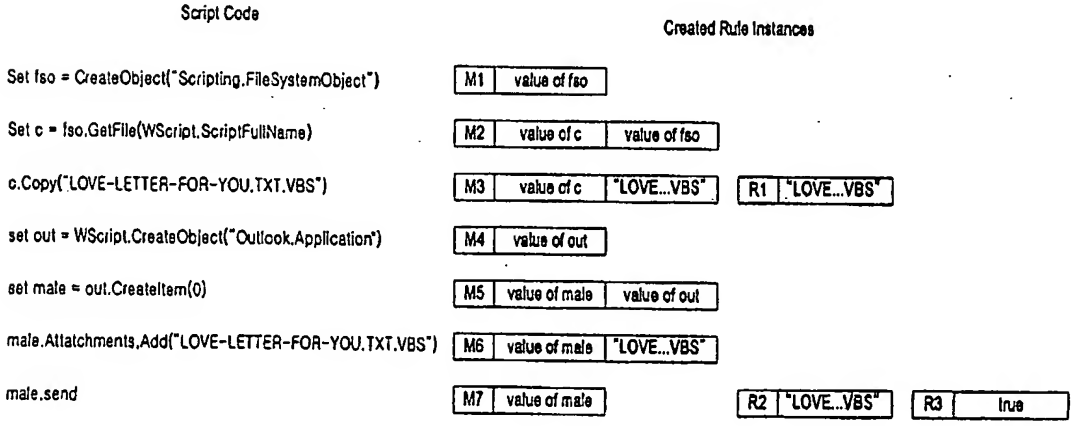
FIG. 10